

JC956 U.S. PTO
10/31/00

11-02-00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 005220.P002

Total Pages 5

First Named Inventor or Application Identifier Dave Parker

Express Mail Label No. EL143569260US

JC918 U.S. PTO
09/10/00



ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. X Specification (Total Pages 35)
(preferred arrangement set forth below)
 - Descriptive Title of the Invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claims
 - Abstract of the Disclosure
3. X Drawings(s) (35 USC 113) (Total Sheets 9)
4. X Oath or Declaration (Total Pages 6)
 - a. Newly Executed (Original or Copy)
 - b. Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) (**Note Box 5 below**)
 - i. DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. Microfiche Computer Program (Appendix)

7. _____ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)

a. _____ Computer Readable Copy

b. _____ Paper Copy (identical to computer copy)

c. _____ Statement verifying identity of above copies

8.	<u> </u>	Assignment Papers (cover sheet & documents(s))
9.	<u> </u>	a. 37 CFR 3.73(b) Statement (where there is an assignee)
	<u> </u>	b. Power of Attorney
10.	<u> </u>	English Translation Document (if applicable)
11.	<u> X </u>	a. Information Disclosure Statement (IDS)/PTO-1449
	<u> X </u>	b. Copies of IDS Citations
12.	<u> </u>	Preliminary Amendment
13.	<u> X </u>	Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14.	<u> </u>	a. Small Entity Statement(s)
		b. Statement filed in prior application, Status still proper and desired
15.	<u> </u>	Certified Copy of Priority Document(s) (if foreign priority is claimed)
16.	<u> X </u>	Other: <u>a copy of the postcard with Certificate of Express Mailing.</u>

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP)
 of prior application No: _____

_____ Customer Number or Bar Code Label _____
 _____ or _____
 (Insert Customer No. or Attach Bar Code Label here)

Country U.S.A. TELEPHONE (408) 720-8598 FAX (408) 720-9397

FEE TRANSMITTAL FOR FY 2001

TOTAL AMOUNT OF PAYMENT (\$) 1,176.00

Complete if Known:

Application No. To be assigned
 Filing Date Herewith
 First Named Inventor Dave Parker
 Group Art Unit To be assigned
 Examiner Name To be assigned
 Attorney Docket No. 005220.P002

Jc918 U.S. PTO
09/703329
10/31/00

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:

Deposit Account Number 02-2666
 Deposit Account Name _____

☐ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

2. ☒ Payment Enclosed:

☒ Check
☐ Money Order
☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
101	710	201	355	Utility application filing fee	<u>710.00</u>
106	320	206	160	Design application filing fee	_____
107	490	207	245	Plant filing fee	_____
108	710	208	355	Reissue filing fee	_____
114	150	214	75	Provisional application filing fee	_____
SUBTOTAL (1)					<u>\$ 710.00</u>

2. EXTRA CLAIM FEES

			Extra Claims	Fee from below	Fee Paid
Total Claims	<u>37</u>	- 20** =	<u>17</u>	X 18.00 =	<u>306.00</u>
Independent Claims	<u>5</u>	- 3** =	<u>2</u>	X 80.00 =	<u>160.00</u>
Multiple Dependent					= _____

**Or number previously paid, if greater; For Reissues, see below.

Large Entity		Small Entity		Fee Description
Fee Code	Fee (\$)	Fee Code	Fee (\$)	
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	**Reissue independent claims over original patent
110	18	210	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) \$ 466.00

FEE CALCULATION (continued)**3. ADDITIONAL FEES**

<u>Large Entity</u>		<u>Small Entity</u>		<u>Fee Description</u>	<u>Fee Paid</u>
<u>Fee Code</u>	<u>Fee (\$)</u>	<u>Fee Code</u>	<u>Fee (\$)</u>		
105	130	205	65	Surcharge - late filing fee or oath	_____
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	_____
139	130	139	130	Non-English specification	_____
147	2,520	147	2,520	For filing a request for reexamination	_____
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	_____
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	_____
115	110	215	55	Extension for response within first month	_____
116	390	216	195	Extension for response within second month	_____
117	890	217	445	Extension for response within third month	_____
118	1,390	218	695	Extension for response within fourth month	_____
128	1,890	228	945	Extension for response within fifth month	_____
119	310	219	155	Notice of Appeal	_____
120	310	220	155	Filing a brief in support of an appeal	_____
121	270	221	135	Request for oral hearing	_____
138	1,510	138	1,510	Petition to institute a public use proceeding	_____
140	110	240	55	Petition to revive unavoidably abandoned application	_____
141	1,240	241	620	Petition to revive unintentionally abandoned application	_____
142	1,240	242	620	Utility issue fee (or reissue)	_____
143	440	243	220	Design issue fee	_____
144	600	244	300	Plant issue fee	_____
122	130	122	130	Petitions to the Commissioner	_____
123	50	123	50	Petitions related to provisional applications	_____
126	240	126	240	Submission of Information Disclosure Stmt	_____
581	40	581	40	Recording each patent assignment per property (times number of properties)	_____
146	710	246	355	For filing a submission after final rejection (see 37 CFR 1.129(a))	_____
149	710	249	355	For each additional invention to be examined (see 37 CFR 1.129(b))	_____
179	710	279	355	Request for Continued Examination (RCE)	_____
169	900	169	900	Request for expedited examination of a design application	_____
Other fee (specify) _____					_____
Other fee (specify) _____					_____
SUBTOTAL (3)					\$ <u>0</u>

*Reduced by Basic Filing Fee Paid

SUBMITTED BY:Typed or Printed Name: Daniel E. OvanezianSignature: Date: 10/31/00Reg. Number: 41,236Telephone Number: 408-720-8300

SCANNED. # 6

UNITED STATES PATENT APPLICATION

FOR

METHOD OF AND APPARATUS FOR NETWORK
ADMINISTRATION

INVENTORS:

Dave Parker
David D. Faraldo II
Jon Prall
Paul Santinelli
Teresa Ramanan
Lance Peterson
Adam Pingel
Mike Deibler

Prepared by:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026

(408) 720-8598

Attorney Docket No.: 005220.P002

"Express Mail" mailing label number: EL143569260US

Date of Deposit: October 31, 2000

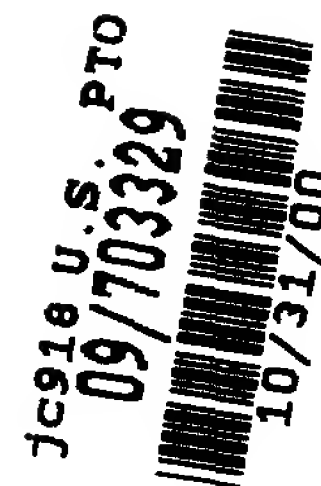
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Conny Willesen

(Typed or printed name of person mailing paper or fee)

Conny Willesen
(Signature of person mailing paper or fee)

10-31-00
(Date signed)



METHOD OF AND APPARATUS FOR NOTIFICATION OF STATE CHANGES IN A MONITORED SYSTEM

FIELD OF THE INVENTION

This invention relates to the field of network administration and, in particular, to notification of state changes in a monitored system on a network.

BACKGROUND

The infrastructure of the Internet may be described in a simplified manner as a collection of computer systems (e.g., hardware and software) that are interconnected by public/private networks (e.g., transmission lines and routers) to enable the transfer of information among them, as illustrated in Figure 1. The Internet infrastructure is an intricate, extremely rapidly growing mixture of complex and disparate hardware systems, networks, and applications. Maintaining knowledge of these components requires expertise (e.g., system administrators and information technology professionals) that is not easily acquired and often difficult to keep. In addition, much of a company's Internet infrastructure may often be running outside of the company's enterprise in that it is hosted at a third party data center or co-location facility.

The disadvantage of hosting a company's infrastructure at a data center is the overhead of trying to monitor, manage, and support that hosted infrastructure. Data centers may not provide any information on systems and

services running from the switchport down. The result is that companies that host may have no critical view into what is actually happening on the infrastructure for which they have invested large amounts of money.

There are several point solutions attempting to remedy this problem. A point solution is a solution that attempts to address a problem from a particular, and often limited, vantage point. Some examples of point solutions include server monitoring software, network monitoring software, or an application monitoring service. None of these point solutions may be sufficient to reliably monitor a site. This may leave companies scrambling to pick and fit together a mixture of disparate, often overlapping, solutions, none of which span and scale to remedy the entire infrastructure hosting problem.

Many of these solutions also grow out of software companies that have little experience in the infrastructure hosting or Internet content creation industry. This may leave their products limited in scope and often burdens the hosting company with installing and managing additional software in their hosted environment. It also may create scaling problems for installing agents for every monitored aspect on every machine in a hosted environment.

Another solution to the infrastructure hosting problem is from a "lights out" point of view in that the solution attempts to "knock the lights out of" the problem in a quick, all encompassing fashion. Companies employing such a solution typically own the equipment, build the applications, monitor and

manage the infrastructure, support the hardware and software, and run the hosted environment. These companies attempt to cover every aspect of the hosting environment and infrastructure support and management problem.

Such attempts may significantly add to their cost of doing business. For

5 example, monitoring of the infrastructure for a do-it-yourself company requires the installation of software agents on the host systems. As such, a company's resources may be consumed for storage, maintenance, and version progressions of such software. Additionally, applications used by these companies tend to be very code intensive and the operating system of the host systems may not be
10 very reliable. Such platforms may not be very scalable or robust and, thus, may not be as desirable.

The overriding problem with these prior solutions is that they focus on attacking infrastructure problems, rather than proactively preventing them.

Such reactive solutions are limited in their effectiveness in that they may not

15 prevent the same problems from recurring and they may not prevent the occurrence of new problems.

SUMMARY OF THE INVENTION

The present invention pertains to a method of and apparatus for administration of a network site. In one embodiment, the method may include monitoring a parameter of a host system for a predetermined event. A notification may be generated upon the occurrence of the predetermined event to a first person in a hierarchy and escalated to a second person in the hierarchy when the first person fails to acknowledge the notification in a time period.

In one embodiment, the apparatus may include a portal to configure an event for a parameter of a host system and a digital processing system coupled to the portal. The digital processing system may receive data indicative of an occurrence of the event and generate a first notification. The apparatus may also include a notification gateway coupled to the digital processing system to transmit the first notification to a first communication device. The digital processing system may generate a second notification to a second communication device if an acknowledgment is not received within a predetermined time.

Additional features and advantages of the present invention will be apparent from the accompanying drawings and from the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which:

Figure 1 illustrates an internetwork architecture.

5 Figure 2A illustrates one embodiment of a network site monitoring system.

Figure 2B illustrates an exemplary table of monitored services and states for embodiments of host parameters.

10 Figure 2C is an exemplary table illustrating threshold levels and corresponding values that may be set for embodiments of host parameters.

Figure 3 illustrates one embodiment of a host satellite system in the form of digital processing system.

Figure 4 illustrates an alternative embodiment of a network site monitoring system.

15 Figure 5 is a block diagram illustrating an exemplary architecture of a monitoring operations center.

Figure 6 illustrates one embodiment of a network site notification system.

Figure 7 illustrates one embodiment of an administration method.

DETAILED DESCRIPTION

In the following description, numerous specific details are set forth such as examples of specific systems, languages, components, etc. in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that these specific details need not be employed to practice the present invention. In other instances, well known materials or methods have not been described in detail in order to avoid unnecessarily obscuring the present invention.

The present invention includes various steps, which will be described below. The steps of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, the steps may be performed by a combination of hardware and software.

The present invention may be provided as a computer program product, or software, that may include a machine-readable medium having stored thereon instructions, which may be used to program a computer system (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks, ROMs, RAMs, EPROMs,

EEPROMs, magnetic or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions.

In one embodiment, a network site monitoring system may be used to provide a means to proactively monitor a business site's services and resources.

5 Various parameters of a host may be configured for monitoring for the occurrence of a predetermined event such as a state change or exceeding a threshold. Upon such occurrence, a notification may be sent to one or more appropriate persons designated by the business site. The notification system may notify the appropriate person for a number of times over a configurable
10 amount of time using various communication means. If that person fails to respond, the system may escalate the notification to another person based on a set of escalation rules. The escalation rules determine who should be notified next in the event that a preceding recipient of a notification fails to respond to a notification with an acknowledgement.

15 In another embodiment, information about host parameters, such as statistical reports and historical trends, may be generated and provided to the business site. In another embodiment, host asset information may be generated to provide a business site with an account of all hardware and software assets in their infrastructure. In yet another embodiment, a portal may be provided to
20 enable a business site to configure the monitoring, escalation, and reporting process and provide access to the generated data.

Figure 2A illustrates one embodiment of a network site monitoring system. The network monitoring system 200 may include various hardware and software components to perform monitoring functions. The network monitoring system 200 includes a business site 210 and a monitoring operations center (MOC) 230. In one embodiment, MOC 230 may be located remotely from business site 210. Alternatively, MOC 230 may be located locally to business site 210. Business site 210 and MOC 230 may be coupled together via extranetwork 220, such as an Internet Protocol (IP) network.

An IP network transmits data in the form of packets that include an address specifying the destination systems for which communication is intended. Business site 210 and MOC 230 may communicate with each other using various protocols, for examples, HTTP, Telnet, NNTP, and FTP. Security layers for managing the security of data transmission may also reside between the application protocols and the lower protocol (TCP/IP) layers, for examples: Secure Sockets Layers (SSL). Alternatively, secure application protocols may be used, for examples, Secure HTTP (HTTPS) and Secure Shell (SSH). These various protocols are known in the art; accordingly, a detailed discussion is not provided herein.

Business site 210 may include one or more computer systems, or hosts, (e.g., hosts 211-213) connected together via intranetwork 215. Three hosts 211-213 are shown only for illustrative purposes. Business site 210 may have more or

less than three hosts. Hosts 211-213 may be configured to perform as servers. In one embodiment, intranetwork 215 is a local area network (LAN). The local area network may be either a wired or wireless network. Alternatively, hosts 211-213 may be coupled together using other types of networks, for example, a metropolitan areas network (MAN) or a wide area network (WAN) with various topologies and transmission mediums.

Business site 210 includes a host satellite system 250 coupled to intranetwork 215. The host satellite system 250 may reside locally at business site 210 to monitor hosts 211-213. Host satellite system 250 may be connected to intranetwork 215 inside of its firewall (not shown). Alternatively, host satellite system 250 may be connected outside of the firewall if the firewall is configured to allow host satellite system 250 access to hosts 211-213. Host satellite system 250 includes monitoring software that monitors performance characteristics and services of hosts 211-213 (e.g., state changes, connection status, etc.), as discussed below. Host satellite system 250 is a digital processing system that may perform various client-server functions.

A host (e.g., host 211) may be configured to provide various services for clients that are accessed through ports of the host connected to intranetwork 215. Types of network services include, for examples, electronic mail using a Simple Mail Transfer Protocol (SMTP), web page display using HTTP, news article distribution using a Network News Transfer Protocol (NNTP), fetching email

from a remote mailbox using a Post Office Protocol-3 (POP3), and text file retrieval for viewer displaying using Gopher, etc. Each service may be configured on an industry standard port or on a custom port. If a service operates with a custom port, then host satellite system 250 may either be

5 preprogrammed with the port information or perform probes to determine a port's configuration.

For example, if host 211 is configured to operate as an HTTP server, host satellite system 250 may attempt to establish a connection (e.g., ping) to industry standard TCP port 80 (or port 443 if HTTPS is used) to determine if it is

10 connected to intranetwork 215. If no reply is received, then port 80 for that particular host 211 is either down or host 211 may be using a different port for the service.

Figure 3 illustrates one embodiment of a host satellite system in the form of digital processing system 300 representing an exemplary workstation, personal computer, server, etc., in which features of the present invention may

15 be implemented.

Digital processing system 300 includes a bus or other communication means 301 for communicating information, and a processing means such as processor 302 coupled with bus 301 for processing information. Digital

20 processing system 300 further includes system memory 304 that may include a random access memory (RAM), or other dynamic storage device, coupled to bus

301 for storing information and instructions to be executed by processor 302.

System memory 304 also may be used for storing temporary variables or other intermediate information during execution of instructions by processor 302.

System memory 304 may also include a read only memory (ROM) and/or other

5 static storage device coupled to bus 301 for storing static information and instructions for processor 302.

A mass storage device 307 such as a magnetic disk or optical disc and its corresponding drive may also be coupled to digital processing system 300 for storing information and instructions. The data storage device 307 may be used
10 to store instructions for performing the steps discussed herein. Processor 302 may be configured to execute the instructions for performing the steps discussed herein. In one embodiment, digital processing system 300 is configured to operate with a LINUX operating system stored on data storage device 307. In alternative embodiments, another operating system may be used, for examples,
15 UNIX, Windows NT, and Solaris.

In one embodiment, digital processing system 300 may also be coupled via bus 301 to a display device 321, such as a cathode ray tube (CRT) or Liquid Crystal Display (LCD), for displaying information to system administrator. For example, graphical and/or textual depictions/indications of system performance
20 characteristics, and other data types and information may be presented to the system administrator on the display device 321. Typically, an alphanumeric

input device 322, including alphanumeric and other keys, may be coupled to bus 301 for communicating information and/or command selections to processor 302. Another type of user input device is cursor control 323, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 302 and for controlling cursor movement on display 321.

A network interface device 325 is also coupled to bus 301. Depending upon the particular design environment implementation, the network interface device 325 may be an Ethernet card, token ring card, or other types of physical attachment for purposes of providing a communication link to support a local area network, for example, for which digital processing system 300 is monitoring. In any event, in this manner, digital processing system 300 may be coupled to a number of clients and/or servers via a conventional network infrastructure, such as a company's Intranet and/or the Internet, for example.

It will be appreciated that the digital processing system 300 represents only one example of a system, which may have many different configurations and architectures, and which may be employed with the present invention. For example, some systems often have multiple buses, such as a peripheral bus, a dedicated cache bus, etc.

In one embodiment, a communication device 326 may also be coupled to bus 301. The communication device 326 may be a modem, or other well-known

interface device, for providing a communication link to a MOC independent of the communication link to which network interface 325 is connected. In this manner, communication device 326 provides a backup link to a MOC if the primary link fails as illustrated by Figure 4.

5 For example, referring to Figure 4, host satellite system 450 may include a modem to enable communication via the Public Switched Telephone Network (PSTN) 425 with MOC 430 independent of the communication link through IP network 420. In an alternative embodiment, other communication means (e.g., wireless network and private voice and/or data network) may be used to enable
10 host satellite system 450 communication with MOC 430 independent of IP network 420.

Referring again to Figure 2A, the monitoring software residing on host satellite system 250 performs both external and internal monitoring of hosts 211-213. For external monitoring, host satellite system 250 monitors network services
15 of a host by accessing the host's ports that are connected to intranetwork 215. As previously discussed, types of network services may include, for examples, SMTP, web page display using HTTP, news article distribution using NNTP, fetching email from a remote mailbox using POP3, and determining whether a particular IP address is accessible using a PING utility. Each service may be
20 configured on an industry standard port or on a custom port. If a service operates with a custom port, then host satellite system 250 may either be

preprogrammed with the port information or make perform searches to determine a port's configuration.

Figure 2B illustrates an exemplary table of monitored services and states. For example, if a host is configured to operate as an HTTP server, the host satellite system may attempt to establish a connection to industry standard TCP port 80 (or port 443 if HTTPS is used) to check the port/service. The host satellite system checks the HTTP service on that port and generates one or more state changes if the service is not operating according to predetermined states, for example, if the answer time is above a threshold value. The test may follow redirects, search for strings and regular expressions, check connection times, and report on certificate expiration times.

If no reply is received, then the host satellite system may determine that the port 80 for that particular host is either down or that a different port is being used for the service. As previously mentioned, a host may support the services listed in Figure 2B and/or custom services assigned to different ports.

Figure 2C is an exemplary table illustrating threshold levels and corresponding values that may be set for embodiments of host parameters. For internal monitoring, the host satellite system logs into a host to monitor the host's resources and evaluate internal states of the host system. In one embodiment, a host's resources may include, for examples, processor, load, disk storage, main memory storage, log files, etc. The internal states of a host may

include, for examples, load on the host 243, processor utilization 242, disk utilization 241, memory utilization 244, number of users connected to the host 245, and number of process running on the host 246. One or more notifications may be generated when an internal state exceeds a corresponding predetermined threshold value as illustrated in Figure 2C. The internal monitoring may include recording of states over time (e.g., the amount of available memory at given time intervals); identification of state changes; and notification of state changes.

In one embodiment, the available disk space 241 of a host system may be monitored and a notification generated if the percentage of available space exceeds one of the threshold values. If a host is considered to have more than 25% of its disk space free during its normal operations, for example, then the host satellite system may be configured to record the amount of available disk space in predetermined time increments (e.g., every 10 minutes); identify a state change when the amount of disk space being used reaches 75%; and generate a warning notification of the state change. In another embodiment, a critical notification may be generated when the amount of disk space being used reaches 90%. The host satellite system stores this information for later collection by the MOC. In one embodiment, the monitoring software may be NetSaint available from Ethan Galstad at <http://www.netsaint.org>. Alternatively, other monitoring software may be used, for examples, HP Openview and Sitescope. In another embodiment, a custom monitoring software may be created.

Referring again to Figure 2A, the data stored on host satellite system 250 may either be pushed or pulled across extranetwork 220 to MOC 230 for processing such as evaluation, notification, and reporting. In one embodiment, for example, host satellite system 250 pushes the stored data across extranetwork 220 to servers at MOC 230. The data may be pushed to different servers, and stored in corresponding databases, depending on the type of data, as discussed below in relation to Figure 5. With either a push or pull methodology, the data may be periodically transferred between host satellite system 250 and MOC 230.

In one embodiment, host satellite system 250 includes a queuing client to store and queue collected data and periodically transmit the data to MOC 230. In an alternative embodiment, host satellite system 250 includes multiple queues with each one configured to store and queue different types of data. For example, one queue may be used for state change data and another queue may be used for time series data. The transmission of data from the multiple queues may be prioritized, for example, all notifications may be set to go to MOC 230 before state change or time series data.

Figure 5 is a block diagram illustrating an exemplary architecture of a monitoring operations center. The architecture may be implemented on one or more servers and corresponding databases. In one embodiment, MOC 530 may include a proxy server 510, a notification gateway 580, a state change server 540, a time series server 550, a reports server 560, a configuration server 570, and a

bus or other communication means 520 for communicating information among them. The servers 540, 550, 560, and 570 may include corresponding databases, for examples: a state change database 545 for storing state change data; a time series database 555 for storing information (e.g., load) over time; a reports database 565 for storing report data; and a configuration database 565 for storing notifications, event handling, trouble tickets, and backup storage, as discussed in detail below. The hardware configuration of the servers may be similar to the digital processing systems discussed above in relation to Figure 3.

MOC 530 may include proxy server 510 to operate as an intermediary between a servers 540-570 and an extranetwork (e.g., extranetwork 220 of Figure 2) to enable security, administrative control, and caching service. Proxy server 510 may be associated with or be part of a gateway server (e.g., gateway server 580) that separates MOC 530 from the extranetwork and a firewall server that protects MOC 530 from outside intrusion. Proxy server 510 may also operate as a cache server. The functions of proxy, firewall, and caching can be in separate server programs or combined in a single program. Different server programs can be in different servers. For example, a proxy server may be in the same machine with a firewall server or it may be on a separate server and forward requests through the firewall. Proxy, firewalls, and caching are well known in the art; accordingly, a detailed discussion is not provided herein.

check delay determines how service checks are initially distributed in an event queue. The use of delays between service checks may help to reduce, or even eliminate, CPU load spikes on a host.

In one embodiment, other types of parameters may be configured, for example, timing parameters. The timing parameters may include, for examples, time between failed checks, check period, and scheduling passes. Check period defines the scheduled time period that a host check is performed. Time between failed checks is the amount of time between the detection of a failure and when the host, service, or satellite is checked again for the same failure. Scheduling passes is the number of seconds per "unit interval" used for timing, for example, in the scheduling queue, re-notifications, etc.

Referring still to Figure 5, servers 540, 550, 560, 570 and their corresponding databases may be used to provide for storage of monitored parameters, notification, escalation, and reporting. Notification server 570 may include a common gateway interface (CGI) that defines the protocol by which notification server 570 interacts with the program that processes the data sent from a host satellite system. Notification gateway 580 is used to generate alerts through various communication means as discussed below in relation to Figure 6.

When a predetermined event occurs, a person designated to receive a notification may receive such notification by the sending of an alert through a

communication channel to a communication device 670, as illustrated in Figure 6.

The communication device may be, for examples, a pager, a telephone, voicemail system, email system with the appropriate transmission protocols used. In one embodiment, for example, communication device 670 may be land-line phone

5 coupled to PSTN 625 and the alert may be transmitted through PSTN 625. In an alternative embodiment, communication device 670 may be a client system

capable of receiving emails that is coupled to IP network 620 and the alert may be transmitted through IP network 620. In yet another embodiment, for

example, communication device 670 may be a wireless phone coupled to wireless

10 network 665 and the alert may be transmitted through wireless network 665. In

an alternative embodiment, other communication devices, and corresponding channels, may be used, for examples, electronic sign boards. Notifications are

not limited to only a single communication device or channel. An alert may be transmitted to multiple communications devices in parallel or in series.

15 With the CGI, a notification server of MOC 630 may serve information that is stored in a format that is not readable by the communication device by presenting such information in a form that is readable communication device 670. The CGI receives the data (e.g., which host had a state change and the particular state that changed) sent from host satellite system 650 to MOC 630 and

20 constructs a message, referred to as an alert, for transmission to communication device 670. Alert programs are known in the art; accordingly a detailed

discussion is not provided. In one embodiment, for example, the TelAlert program available from Telamon of Oakland, California may be used.

Referring again to Figure 5, notifications may be set up with various notification and escalation parameters that determine hierarchies and priorities.

5 For example, a notification may be configured for transmission to one or more communications devices of a particular person. If that person does not acknowledge the notification in a predetermined period of time, a set of escalation parameters may be established to send the notification to the communication device(s) of another person or persons. Furthermore, the
10 escalation of the notification may be prioritized based on a particular type of notification.

In one embodiment, notification parameters may include, for examples, notify on critical, notify on host down, notify on recovery, and notify on warning, time between notifications. The notify on critical parameter determines
15 whether a contact is notified if a service is in a critical state. The notify on host down parameter determines whether notifications are sent to any contacts if the host is in a down state. The notify on recovery parameter determines whether notifications are sent to any contacts if the host is in a recovery state. The notify on warning parameter determines whether a contact will be notified if a service
20 is in either a warning or an unknown state. Time between notifications is the

number of time units to wait before re-notifying a contact that a server is still down.

In one embodiment, the system may be configured to prevent the generation of multiple notifications for host state changes that are dependent upon one another. For example, a host probe and a service probe are dependent upon each other. If a host is down then service probes of that host would generate multiple state changes due to the non-operation of all the services of that host. In order to avoid redundant dependency notifications, those services probes that are already known to be dependent upon the same host probe may be disabled. Alternatively, state changes may be analyzed at the MOC to avoid transmission of dependent notifications.

In one embodiment, an analysis engine may be used to provide suggestions of probable causes of and solutions to problems evidenced by state changes. The expertise of individuals that have diagnosed and solved problems is used to build a database relating problems with causes and solutions. The analysis engine evaluates the state change that occurs based on the stored database of knowledge and provides a list of possible causes that may be attributable to the state change along with a possible solution.

As previously discussed, if a notification is not acknowledged, it may be escalated based a set of escalation rules. The escalation rules may be based on configurable parameters such acknowledgment wait (i.e., the time delay between

Attorney Docket No. 005220.P002

C's phone if neither person A nor B acknowledge the notification within a similar or different predetermined time period (e.g., 30 minutes). During those time periods (e.g., 90 minutes), the configuration database may operate as a backup database in case of failure of the state change server/database. As such, if state change server 540 fails after person B is notified, the notification server 570 may use the data stored in the configuration database 575 to notify person C if person B has not acknowledged within the allotted time.

In one embodiment, notification server 570 includes an event handler script that recognizes when a notification is complete, determines whether the notification is completed successful, and analyzes whether the escalation rules were followed. A notification may be deemed to be successful based on a predetermined standard, for example, a person in the notification hierarchy acknowledged a notification. In one embodiment, the predetermined standard for a successful notification may be configured by the business site. If the notification is deemed not to be successfully completed, then an alert may be sent to notifies a person associated with MOC 530 of the notification failure. In this manner, that person may decide what, if any, additional actions may be taken including attempting to correct the problem (that caused the state change) for the customer.

In one embodiment, report server 560 may generate real-time and historical reports of the data received from the host satellite system about the

business site' infrastructure. In one embodiment, the reports may be stored in report database 565 as a result of a predetermined query (e.g., daily, weekly, monthly, etc.). The report database 565 may be accessed through configuration portal 590. Configuration interface 590 may generate reports based on pre-stored or configurable queries. Alternatively, a user can specify a query based on a specific infrastructure view (e.g., monitor, host, port, etc.). In addition, the reporting format of collected data may also be configured, for examples, graphics of state change, graphs over time, number of notifications in progress, how many probes into the business site are reporting a bad status, etc. It should be noted that all of the parameters discussed herein in relation to Figures 2-7 may either be configured by a business site or by a MOC.

Figure 7 illustrates one embodiment of an administration method. In one embodiment, a parameter of a host system is monitored for a predetermined event, step 710. The predetermined event may be a state change of the monitored parameter. Data that includes the state change data may be received by a monitoring operations center, step 720. The monitoring operations center may generate a notification of the state change upon the occurrence of the predetermined event with the notification sent to a first person in a hierarchy, step 730. In one embodiment, a possible cause of the occurrence and a possible corrective action may be provided, step 735.

005220.P002

If an acknowledgement is not received with a certain configurable time period, step 740, then the notification may be escalated to another person in the hierarchy, step 750. The escalation may be repeated if an acknowledgment is not received within a configurable time period. In one embodiment, a trouble ticket
5 may be generated at a predetermined point in the hierarchy to track the escalation, step 755.

In one embodiment, a determination may be made as to whether the notification is completed successful, step 760. A report may be generated based on the data received by the monitoring operations center, step 770.

10 Referring again to Figure 2, host satellite system 250 may also be used to monitor asset parameters of a business site's infrastructure 210. The asset parameters are those that may be used to track and identify the assets of business site 210 that may be used by, for example, an accounting department. The asset parameters may include, for examples: serial number of a host; model
15 number of a host; rack location; asset ID; lease ID; operating system type; the number of processors the host has installed; processor type.

In one embodiment, the steps discussed above may be implemented with an interpreter program. An interpreter is a language processor that analyzes a program (i.e., lines of code) and then carries out the specified actions (processes
20 instructions) at the time of execution, rather than producing a machine-code translation to be executed later (as with a compiler). In one embodiment, the

steps discussed above are coded using Perl. In an alternative embodiment, other programming languages may be used.

The methods and apparatuses described herein may provide businesses a means to proactively monitor their site's resources from a remote location. The result of this may be the prevention of problems before they happen and the reduction in the need for reactive problem solving. In addition, with no agents to install on client host machines, there may be no maintenance issues with version progressions for a business. Additionally, such a solution may eliminate large footprints that consume the valuable system resources of a business.

In addition, statistical reports, historical trend information, and asset management may also be provided to the business site. Such data may allow for more informed business decisions and drive down costs of unnecessary hardware purchases and the number of required support professionals.

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method, comprising:
 - monitoring a parameter of a host system for a predetermined event;
 - generating a notification upon the occurrence of the predetermined event to a first person in a hierarchy; and
 - escalating the notification to a second person in the hierarchy when the first person fails to acknowledge the notification in a time period.
2. The method of claim 1, further comprising determining whether the notification is successful.
3. The method of claim 1, wherein the predetermined event is receipt of a state change of the parameter.
4. The method of claim 1, wherein the predetermined event is exceeding a threshold value set for the parameter.
5. The method of claim 1, further comprising generating the notification a number of times for an amount of time.
6. The method of claim 5, wherein the number of times, the amount of time, and the time period are configurable.

- 1 7. The method of claim 1, wherein the parameter is monitored using a
2 satellite system located locally to the host system and wherein the
3 notification is generated remotely from the host system.
- 1 8. The method of claim 7, further comprising:
2 receiving data about the predetermined event from a satellite
3 system by a monitoring operations center and wherein the notification is
4 generated by the monitoring operations center.
- 1 9. The method of claim 1, further comprising providing a possible
2 cause of the predetermined event occurrence.
- 1 10. The method of claim 1, where escalation is based on a set of rules.
- 1 11. The method of claim 10, wherein the set of rules is based on a time
2 delay between the notification and the acknowledgement.
- 1 12. The method of claim 10, wherein the set of rules is based on the
2 state change.
- 1 13. The method of claim 10, wherein the set of rules is based on
2 schedules of the first and second persons.
- 1 14. The method of claim 1, wherein the notification is generated and
2 escalated automatically.
- 1 15. The method of claim 1, further comprising generating a trouble
2 ticket at a predetermined point in the hierarchy to track the escalation.

- 1 16. The method of claim 1, wherein the parameter is a service of the
2 host system.
- 1 17. The method of claim 1, wherein the parameter is a utilization of a
2 component of the host system.
- 1 18. The method of claim 17, further comprising:
2 monitoring additional parameters of the host system, wherein the
3 additional parameters include a service of the host system; and
4 eliminating a redundant notification based on dependent
5 parameters of the host system.
- 1 19. The method of claim 17, further comprising determining an asset of
2 the host system.
- 1 20. A machine readable medium having stored thereon instructions,
2 which when executed by a processor, cause the processor to perform the
3 following:
4 monitoring a parameter of a host system for a predetermined
5 event;
6 generating a notification upon the occurrence of the predetermined
7 event to a first person in a hierarchy; and
8 escalating the notification to a second person in the hierarchy when
9 the first person fails to acknowledge the notification in a time period.
- 1 21. The machine readable medium of claim 18, wherein the
2 predetermined event is receipt of a state change of the parameter.

1 22. The machine readable medium of claim 18, wherein the processor
2 further performs generating the notification a number of times for an
3 amount of time.

1 23. The machine readable medium of claim 18, wherein the number of
2 times, the amount of time, and the time period are configurable.

1 24. The machine readable medium of claim 18, wherein the processor
2 further performs providing a suggestion as to a cause of the
3 predetermined event occurrence.

1 25. The machine readable medium of claim 18, wherein the processor
2 further performs generating a trouble ticket at a predetermined point in
3 the hierarchy to track the escalation.

1 26. An apparatus, comprising:
2 means for monitoring a parameter of a host system for a
3 predetermined event;
4 means for generating a notification upon the occurrence of the
5 predetermined event to a first person in a hierarchy; and
6 means for escalating the notification to a second person in the
7 hierarchy when the first person fails to acknowledge the notification in a
8 time period.

1 27. The apparatus of claim 26, further comprises means for
2 determining whether the notification is successful.

1 28. The apparatus of claims 26, further comprising:

2 means for generating the notification a number of times for an
3 amount of time.

1 29. The apparatus of claim 26, further comprising:

2 means for generating a trouble ticket at a predetermined point in
3 the hierarchy to track the escalation.

1 30. An apparatus, comprising:

2 a portal to configure an event for a parameter of a host system;
3 a digital processing system coupled to the portal, the digital
4 processing system to receive data indicative of an occurrence of the event
5 and generate a first notification; and

6 a notification gateway coupled to the digital processing system to
7 transmit the first notification to a first communication device, the digital
8 processing system to generate a second notification to a second
9 communication device if an acknowledgment is not received within a
10 predetermined time.

1 31. The apparatus of claim 30, wherein the notification gateway
2 transmits the second notification to the second communication device.

1 32. The apparatus of claim 30, wherein the digital processing system
2 comprises at least one server.

1 33. The apparatus of claim 30, further comprising a proxy server
2 coupled to the digital processing system.

1 34. A system, comprising:

2 a host satellite system coupled to a first network;
3 a plurality of communication devices; and
4 a monitoring operations center coupled to the first network, the
5 monitoring operations center comprising:
6 a portal to configure an event for a parameter of a host
7 system;
8 a digital processing system coupled to the portal, the digital
9 processing system to receive data indicative of an occurrence of the
10 event on the first network and generate a first notification; and
11 a notification gateway coupled to the digital processing
12 system to transmit the first notification to one of the plurality of
13 communication devices, the digital processing system to generate a
14 second notification to another of the plurality of communication
15 devices if an acknowledgment is not received within a
16 predetermined time.

1 35. The system of claim 34, wherein the first notification is transmitted
2 on the first network.

1 36. The system of claim 34, further comprising a second network and
2 wherein the first notification is transmitted on the second network.

1 37. The system of claim 35, wherein the first network is an internet
2 protocol network and the second network is a telephone network.

ABSTRACT

A method and apparatus is described for monitoring, notification, and reporting of the status of a business site's infrastructure. The monitoring captures pertinent health and status information of hosts using a satellite system located locally to the hosts. This information serves as a basis for reports that the business site may generate about the hosts. Thresholds may be set on monitored parameters of a host and feed into an acknowledgment based notification process based on a set of escalation parameters that triggers alerts to persons designated by the business site. Real-time and historical of the infrastructure data reports may be generated. An infrastructure's assets may also be tracked.

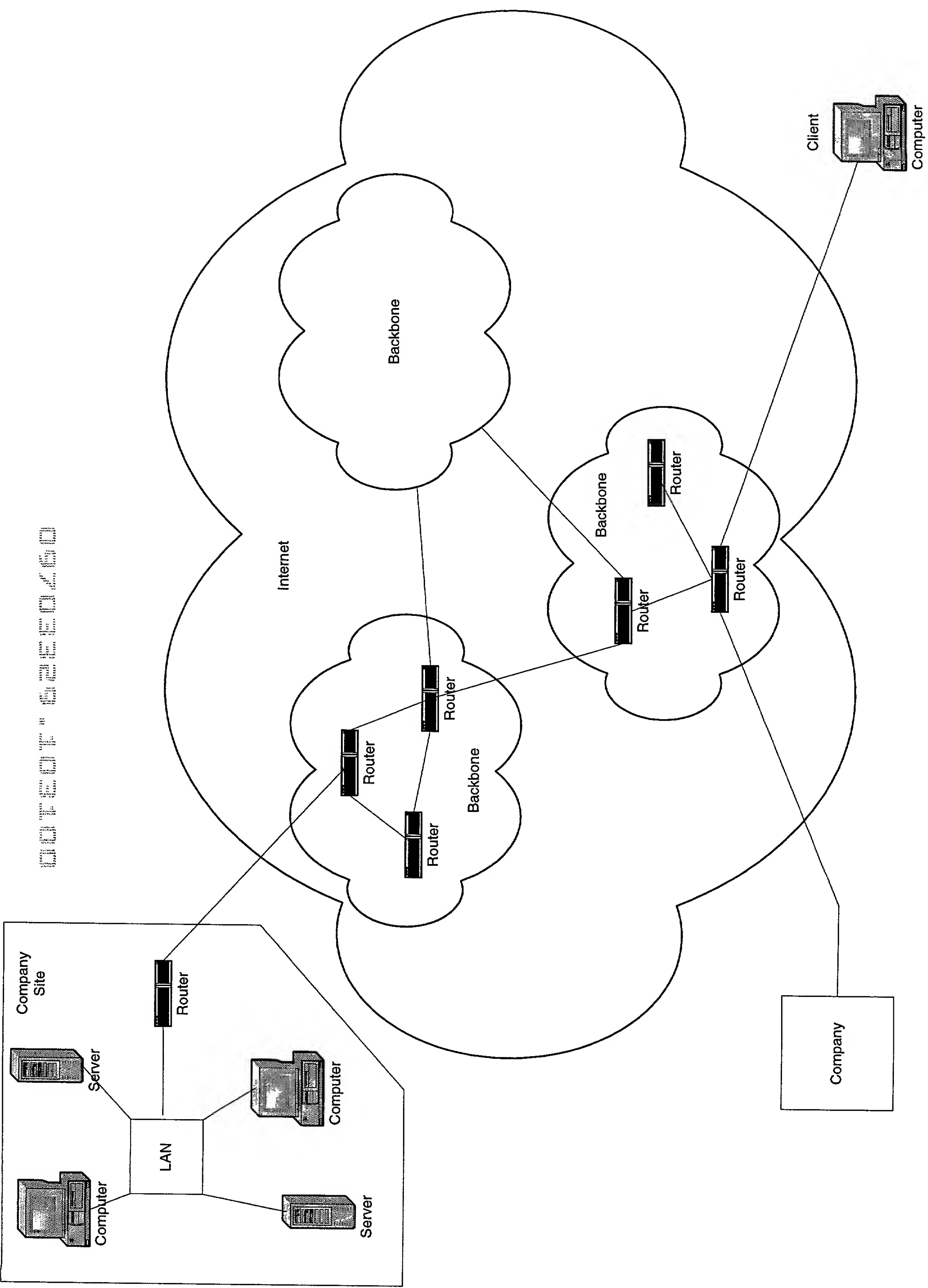
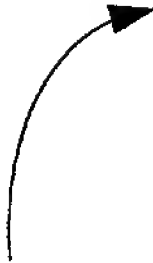


Figure 1



correct" 0000000000

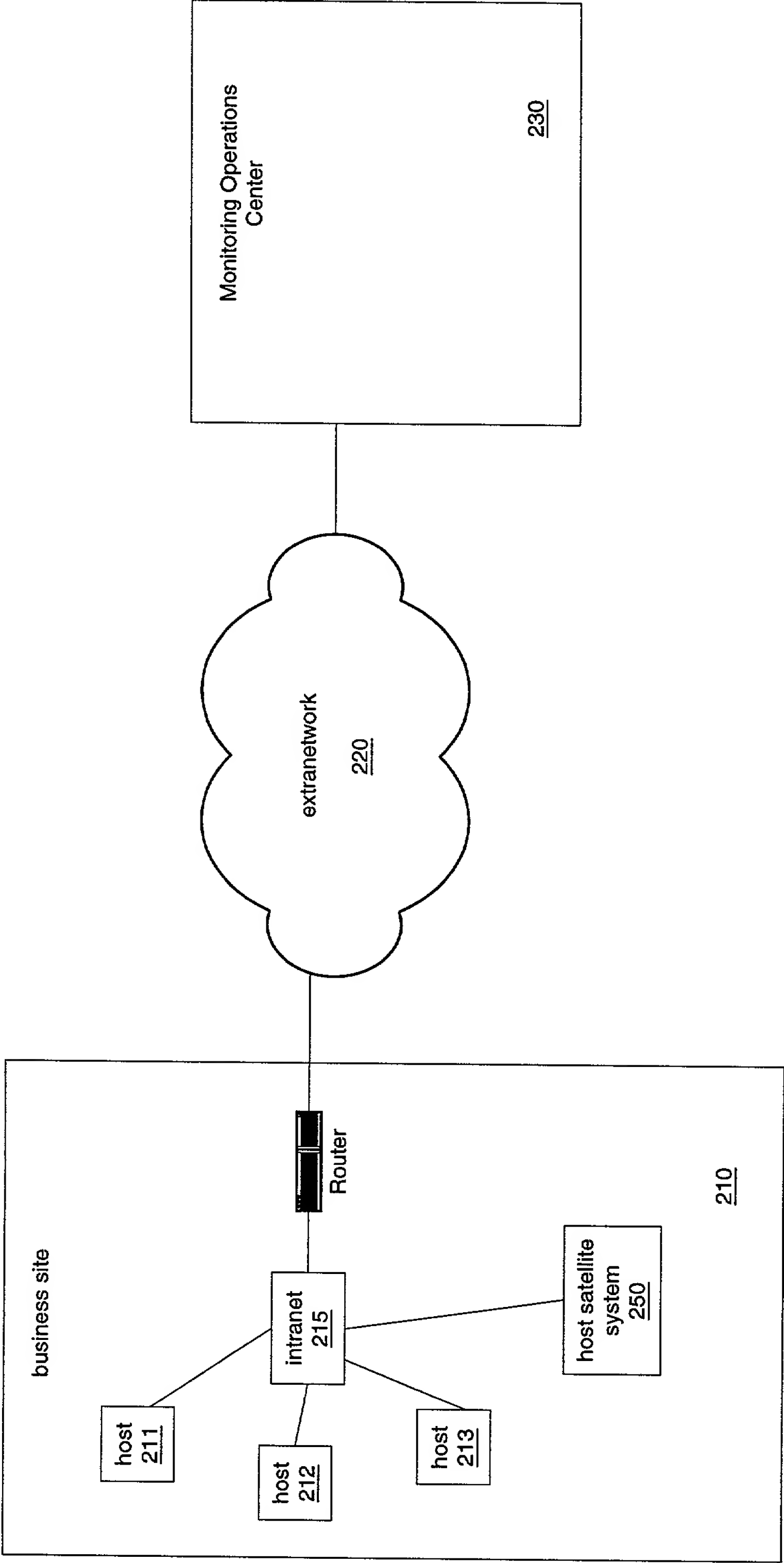


Figure 2A

Figure 2B

PARAMETER	THRESHOLD LEVELS	THRESHOLD VALUES
Disk Utilization	OK	< 75%
	Warning	75%
	Critical	90%
Processor Utilization	OK	< 70%
	Warning	70%
	Critical	85%
Load	OK	< 0.8
	Warning	0.8
	Critical	1
Memory Utilization	OK	< 20%
	Warning	20% free
	Critical	10% free
Swap Space	OK	< 20%
	Warning	20% free
	Critical	10% free
Number of Users	OK	< 10 users
	Warning	10 users
	Critical	20 users
Number of Processes	OK	< 400 processes
	Warning	400 processes
	Critical	700 processes

Figure 2C

Digital Processing System

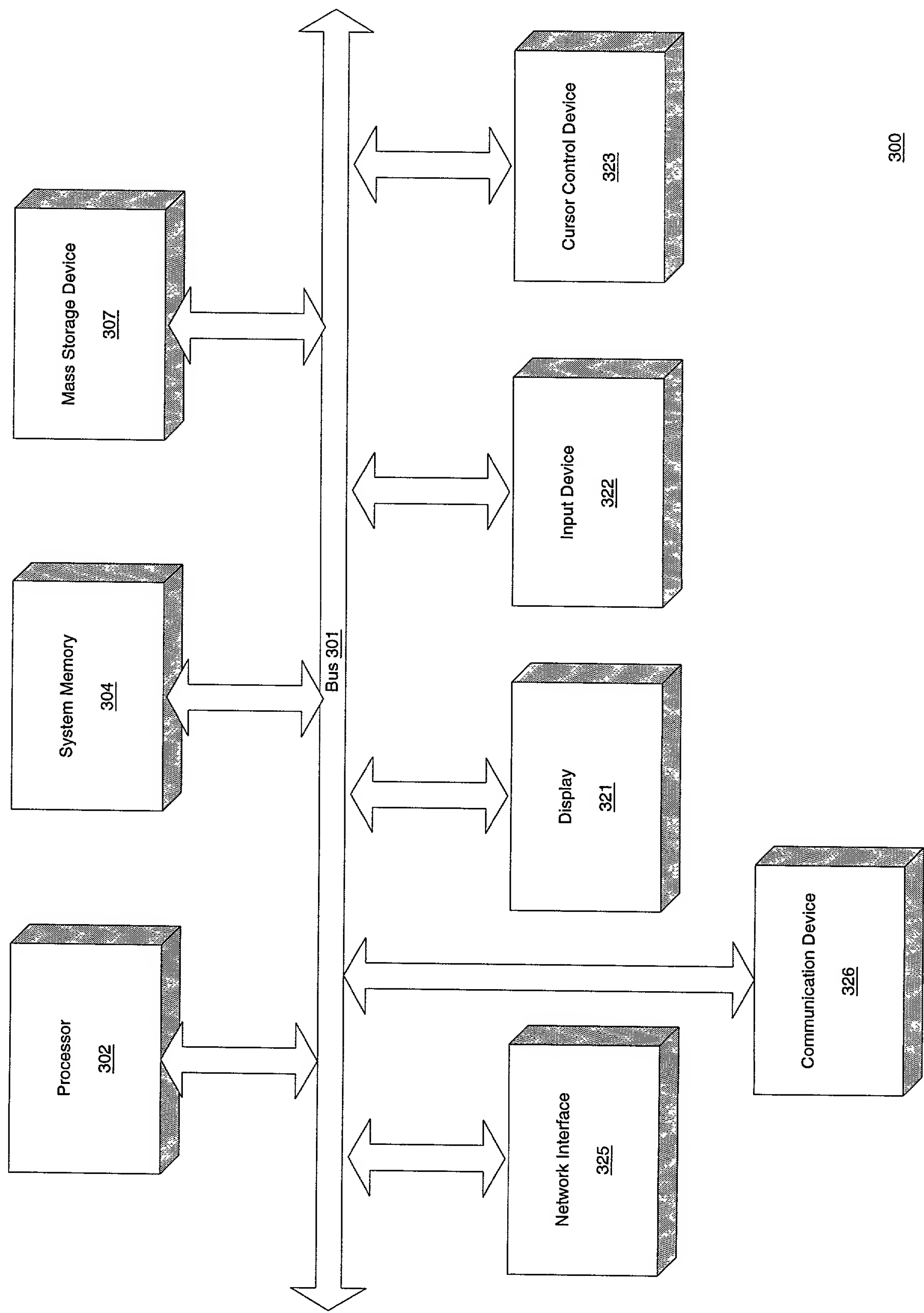


Figure 3

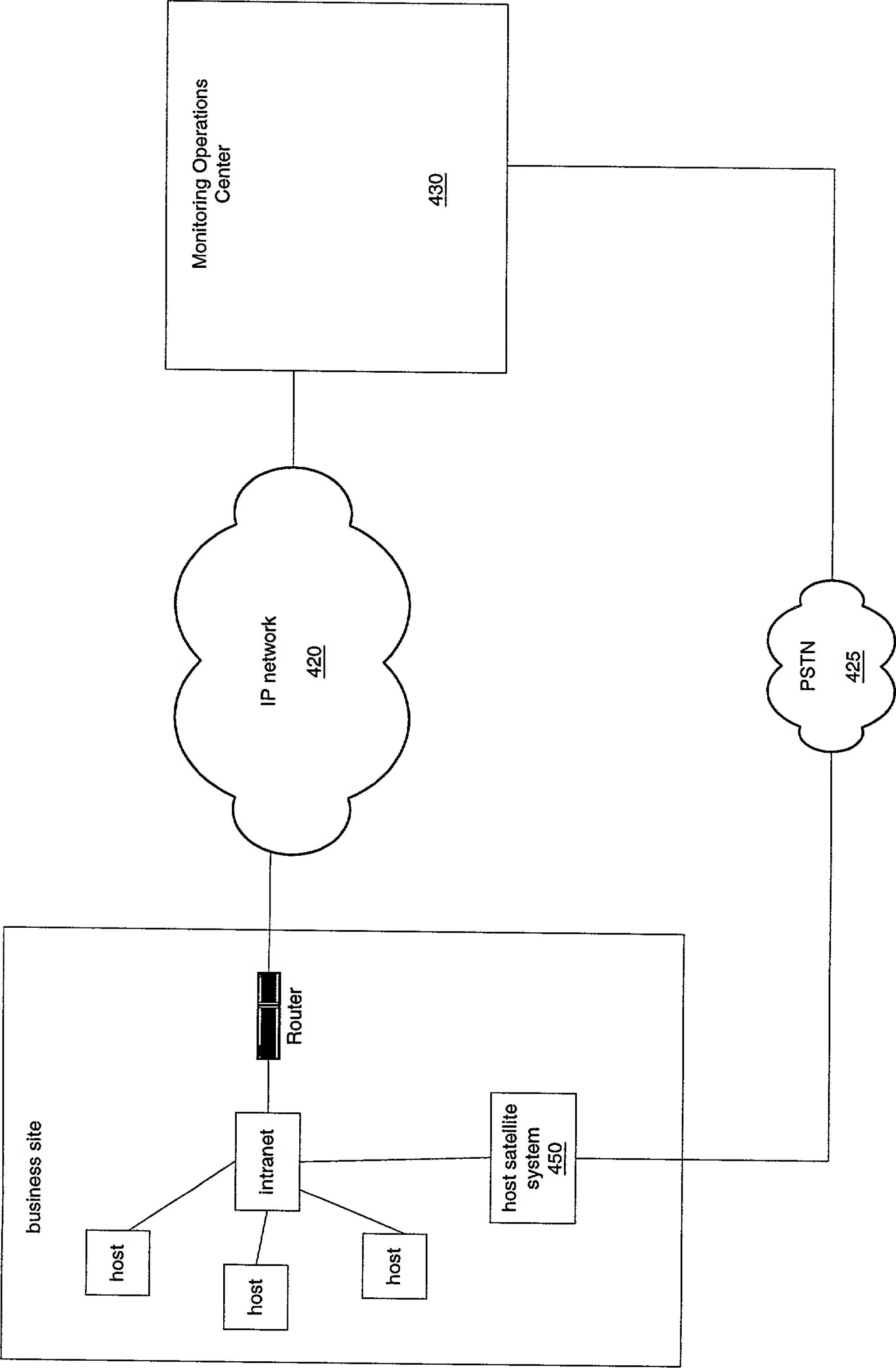


Figure 4

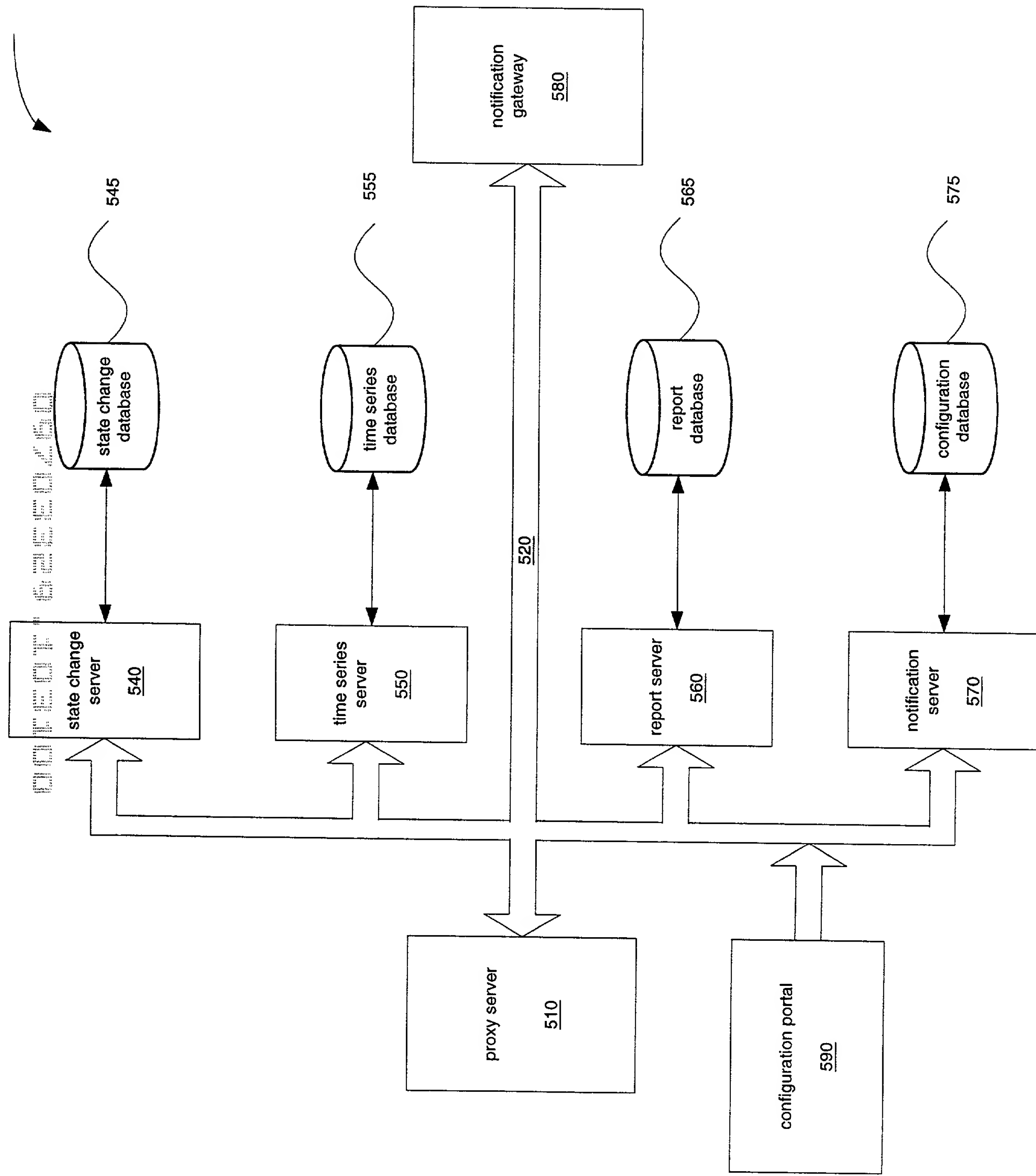


Figure 5

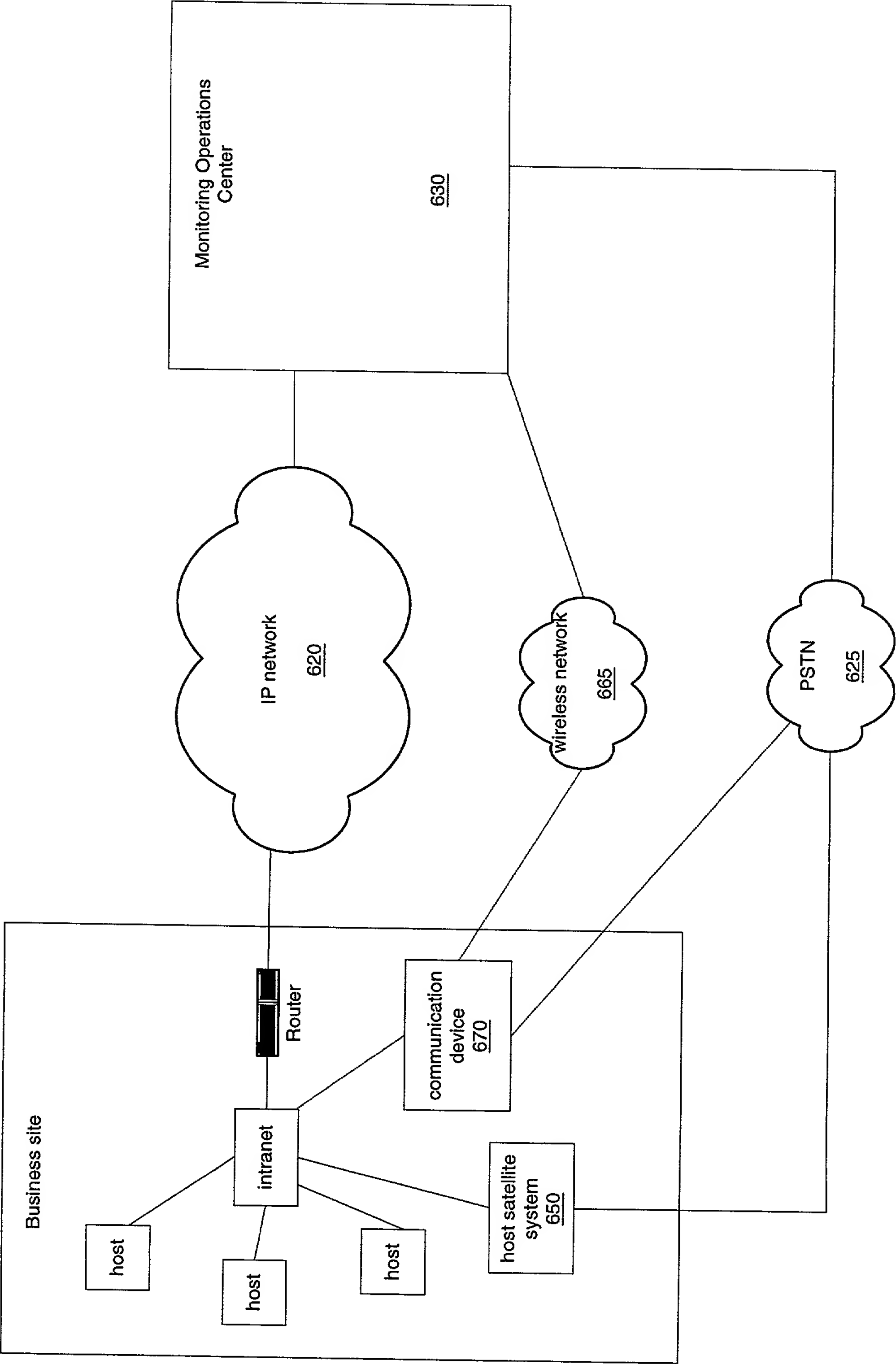


Figure 6

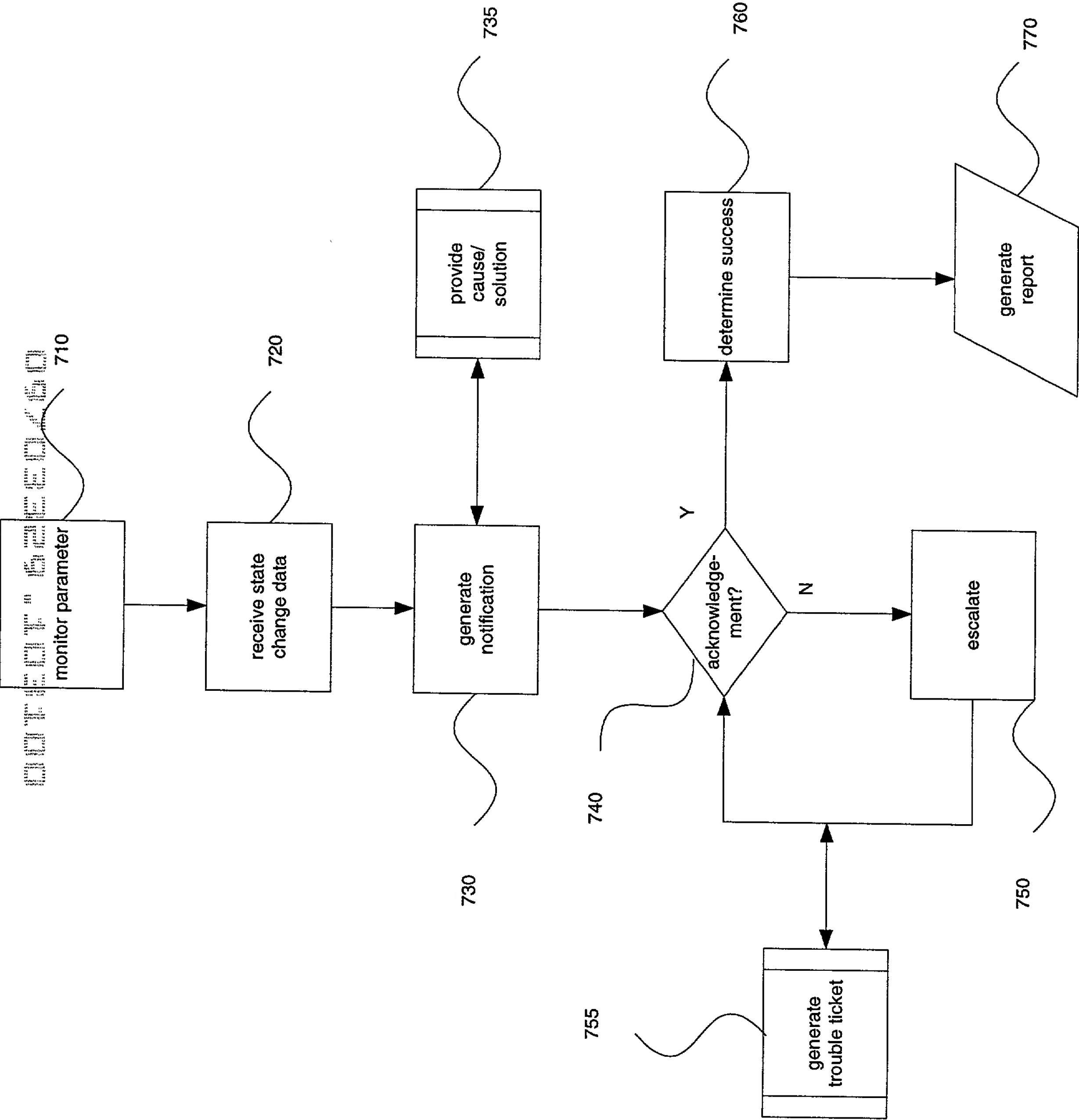


Figure 7

Attorney's Docket No.: 005220.P002

Patent

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
Method Of And Apparatus For Network Administration

the specification of which

X is attached hereto.
_____ was filed on (MM/DD/YYYY) _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on (MM/DD/YYYY) _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

OFFICE OF THE ATTORNEY GENERAL

Prior Foreign Application(s)

Priority
Claimed

<u>(Number)</u>	<u>(Country)</u>	<u>(Foreign Filing Date - MM/DD/YYYY)</u>	<u>Yes</u>	<u>No</u>
<u>(Number)</u>	<u>(Country)</u>	<u>(Foreign Filing Date - MM/DD/YYYY)</u>	<u>Yes</u>	<u>No</u>
<u>(Number)</u>	<u>(Country)</u>	<u>(Foreign Filing Date - MM/DD/YYYY)</u>	<u>Yes</u>	<u>No</u>

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

<u>(Application Number)</u>	<u>(Filing Date – MM/DD/YYYY)</u>
<u>(Application Number)</u>	<u>(Filing Date – MM/DD/YYYY)</u>

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

<u>(Application Number)</u>	<u>(Filing Date – MM/DD/YYYY)</u>	<u>(Status -- patented, pending, abandoned)</u>
<u>(Application Number)</u>	<u>(Filing Date – MM/DD/YYYY)</u>	<u>(Status -- patented, pending, abandoned)</u>

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Daniel E. Ovanezian, BLAKELY, SOKOLOFF, TAYLOR &
(Name of Attorney or Agent)
ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct
telephone calls to Daniel E. Ovanezian, (408) 720-8300.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Dave Parker

Inventor's Signature _____ Date _____

Residence _____ (City, State) _____ Citizenship _____ (Country) _____

Post Office Address _____

Full Name of Second/Joint Inventor David D. Faraldo II

Inventor's Signature _____ Date _____

Residence Foster City, California _____ (City, State) _____ Citizenship U.S.A. _____ (Country) _____

Post Office Address 546 Cutwater Lane _____
Foster City, California 94404 _____

Full Name of Third/Joint Inventor Jon Prall

Inventor's Signature _____ Date _____

Residence _____ (City, State) _____ Citizenship _____ (Country) _____

Post Office Address _____

Full Name of Fourth/Joint Inventor Paul Santinelli

Inventor's Signature _____ Date _____

Residence _____ (City, State) _____ Citizenship _____ (Country) _____

Post Office Address _____

OFFICE OF THE SECRETARY OF COMMERCE

Full Name of Fifth/Joint Inventor Teresa Ramanan

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

Full Name of Sixth/Joint Inventor Lance Peterson

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

Full Name of Seventh/Joint Inventor Adam Pingel

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

Full Name of Eighth/Joint Inventor Mike Deibler

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Florin Corie, Reg. No. 46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, Reg. No. 46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Sanjeet Dutta, Reg. No. 46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 37,374; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Libby N. Ho, Reg. No. 46,774; Willmore F. Holbrow III, Reg. No. 41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W. Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; George Brian Leavell, Reg. No. 45,436; Kurt P. Leyendecker, Reg. No. 42,799; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Robert G. Litts, Reg. No. 46,876; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Robert B. O'Rourke, Reg. No. 46,972; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Gregg A. Peacock, Reg. No. 45,001; Marina Portnova, Reg. No. 45,750; William F. Ryann, Reg. No. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Tom Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. 46,322; Thomas C. Webster, Reg. No. 46,154; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Firasat Ali, Reg. No. 45,715; Justin M. Dillon, Reg. No. 42,486; Thomas S. Ferrill, Reg. No. 42,532; and Raul Martinez, Reg. No. 46,904, my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and James R. Thein, Reg. No. 31,710, my patent attorney with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56 Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) Prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

- (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
- (2) It refutes, or is inconsistent with, a position the applicant takes in:
 - (i) Opposing an argument of unpatentability relied on by the Office, or
 - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

- (1) Each inventor named in the application;
- (2) Each attorney or agent who prepares or prosecutes the application; and
- (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.